



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/442,727	11/18/1999	SADAHARU SATO	450100-02171	6321
20999	7590	02/26/2004	EXAMINER	
FROMMER LAWRENCE & HAUG 745 FIFTH AVENUE- 10TH FL. NEW YORK, NY 10151			VAUGHAN, MICHAEL R	
			ART UNIT	PAPER NUMBER
			2131	17
DATE MAILED: 02/26/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/442,727	SATO, SADAHARU	
Examiner	Art Unit		
Michael R Vaughan	2131		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 15 December 2003.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-8 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 1-8 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 10.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____ .

Detail Action

Response to Arguments

Applicant's arguments with respect to claim 1-8 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Szczutkowski et al. (USP 4,817,146) in view of Cookson et al (USP 5,896,454).

As per claim 1, Szczutkowski et al. teach:

A cipher processing circuit for enciphering data (column 4, lines 42-66);

A transmission circuit for adding the enciphering information to the data enciphered in the cipher processing circuit (see FIG. 1);

Transmitting the result to the serial interface bus (column 8, lines 60-63);

Confirming the continuity of the cipher mode (column 7, lines 5-40 and column 8, lines 20-40);

Transmitting in a different cipher mode when a discontinuity is confirmed (column 20, lines 16-36).

Szczutkowski et al do not teach that one of the cipher modes is a copy once prohibition mode wherein the data cannot be reproduced more than once. Cookson et al teach a copy once prohibition mode wherein the data cannot be reproduced more than once (Fig 2 and column 4, lines 26-32). It is advantageous to provide an additional mode of copying to allow one to make a backup of an original storage of data. This allows a legitimate owner of a piece of data to make a backup copy. In addition it is desirable to prevent a malicious user from making multiples copies from a copy.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cookson et al within the system of Szczutkowski et al because it would allow the system to authorize a one time copy so that a backup can be made of the original piece of data, while preventing illegal subsequent copies from being made from the copy.

As per claim 2, Szczutkowski et al. teach setting the enciphering information in a predetermined region of a header of the packet (column 17, lines 10-12 and column 19, lines 34-51).

As per claim 3, Szczutkowski et al. teach:

A holding means in which information of at least one cipher mode is set (FIG. 1);
A control means for specifying a mode to encipher (FIG. 1);

A cipher processing circuit including a cipher mode selection circuit and a cipher engine circuit for enciphering data and outputting data (FIG. 1 and column 7, lines 5-45);

A transmission circuit for adding the enciphering information to the enciphered data (FIG. 1);

Transmitting the result to the serial interface bus (column 8, lines 60-63);

Confirming the continuity of the cipher mode (column 7, lines 5-40 and column 8, lines 20-40);

Transmitting in a different cipher mode when a discontinuity is confirmed (column 20, lines 16-36).

Szczutkowski et al do not teach that one of the cipher modes is a copy once prohibition mode wherein the data cannot be reproduced more than once. Cookson et al teach a copy once prohibition mode wherein the data cannot be reproduced more than once (Fig 2 and column 4, lines 26-32). It is advantageous to provide an additional mode of copying to allow one to make a backup of an original storage of data. This allows a legitimate owner of a piece of data to make a backup copy. In addition it is desirable to prevent a malicious user from making multiples copies from a copy.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cookson et al within the system of Szczutkowski et al because it would allow the system to authorize a one time copy so that a backup can be made of the original piece of data, while preventing illegal subsequent copies from being made from the copy.

As per claim 4, Szczutkowski et al. teach setting the enciphering information in a predetermined region of a header of the packet (column 17, lines 10-12 and column 19, lines 34-51).

As per claim 5, Szczutkowski et al. teach:

A storing means (FIG. 1);

A holding means in which information of at least one cipher mode is set (FIG. 1);

A control means for specifying a mode to encipher (FIG. 1);

A cipher processing circuit including a cipher mode selection circuit for selecting cipher mode information specified by the control means from the holding means and a cipher engine (DES) circuit for enciphering the data to be transmitted in the cipher mode selected and outputting the enciphered data (FIG. 1 and column 7, lines 5-45);

A first transmission circuit for generating time information (column 17, lines 3-47) to output received data on a receiving side to an application side (column 11, lines 43-48);

A second transmission circuit for reading enciphered data (FIG. 1), generating packet data (FIG. 1), setting enciphering information in a packet header (column 17, lines 10-12 and column 19, lines 34-51) and transmitting the result to a serial interface bus (column 8, lines 60-63), confirming the continuity of the cipher mode (column 7, lines 5-40 and column 8, lines 20-40), and transmitting in a different cipher mode when a discontinuity is confirmed (column 20, lines 16-36).

Szczutkowski et al do not teach that one of the cipher modes is a copy once prohibition mode wherein the data cannot be reproduced more than once. Cookson et al teach a copy once prohibition mode wherein the data cannot be reproduced more than once (Fig 2 and column 4, lines 26-32). It is advantageous to provide an additional mode of copying to allow one to make a backup of an original storage of data. This allows a legitimate owner of a piece of data to make a backup copy. In addition it is desirable to prevent a malicious user from making multiples copies from a copy.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cookson et al within the system of Szczutkowski et al because it would allow the system to authorize a one time copy so that a backup can be made of the original piece of data, while preventing illegal subsequent copies from being made from the copy.

As per claim 6, Szczutkowski et al. teach:

A cipher processing circuit for enciphering data to be transmitted by a predetermined cipher mode (column 7, lines 5-45) at the time of transmission and deciphering the received enciphered data based on the enciphering information included in the received packet data (column 19, line 34 – column 20, line 36);

A transmission circuit for adding enciphering information to the enciphered data (column 19, lines 34-51 and column 17, lines 10-12), transmitting result to a serial interface bus (column 8, lines 60-63), confirming the continuity of the cipher mode

(column 7, lines 5-40 and column 8, lines 20-40), and transmitting in a different cipher mode when a discontinuity is confirmed (column 20, lines 16-36).

Szczutkowski et al do not teach that one of the cipher modes is a copy once prohibition mode wherein the data cannot be reproduced more than once. Cookson et al teach a copy once prohibition mode wherein the data cannot be reproduced more than once (Fig 2 and column 4, lines 26-32). It is advantageous to provide an additional mode of copying to allow one to make a backup of an original storage of data. This allows a legitimate owner of a piece of data to make a backup copy. In addition it is desirable to prevent a malicious user from making multiples copies from a copy.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cookson et al within the system of Szczutkowski et al because it would allow the system to authorize a one time copy so that a backup can be made of the original piece of data, while preventing illegal subsequent copies from being made from the copy.

As per claim 7, Szczutkowski et al. teach setting the enciphering information in a predetermined region of a header of the packet (column 17, lines 10-12 and column 19, lines 34-51).

As per claim 8, Szczutkowski et al. teach:

A first storing means (FIG. 6);

A second storing means (FIG. 6);

A holding means in which information of at least one cipher mode is set (FIG. 1);

A control means for specifying a mode to encipher (FIG. 1);

A first reception circuit for storing time information, enciphered data, and the enciphering information from received packets (FIG. 1, 2, 6, and column 20, lines 36-40);

A second reception circuit for outputting enciphering information and enciphered data to an application based on time information (FIG. 1, 2, 6, and column 21, lines 58-63 and column 17, lines 5-48);

A cipher processing circuit including a cipher mode detection circuit (column 20, lines 16-36);

A cipher mode selection circuit (column 7, lines 31-45);

A cipher engine for enciphering and deciphering (FIG. 1);

A first transmission circuit for generating time information (column 17, lines 3-47) to output received data on a receiving side to an application side (column 11, lines 43-48);

A second transmission circuit for reading enciphered data (FIG. 1), generating packet data (FIG. 1), setting enciphering information in a packet header (column 17, lines 10-12 and column 19, lines 34-51) and transmitting the result to a serial interface bus (column 8, lines 60-63), confirming the continuity of the cipher mode (column 7, lines 5-40 and column 8, lines 20-40), and transmitting in a different cipher mode when a discontinuity is confirmed (column 20, lines 16-36).

Szczutkowski et al do not teach that one of the cipher modes is a copy once prohibition mode wherein the data cannot be reproduced more than once. Cookson et al teach a copy once prohibition mode wherein the data cannot be reproduced more than once (Fig 2 and column 4, lines 26-32). It is advantageous to provide an additional mode of copying to allow one to make a backup of an original storage of data. This allows a legitimate owner of a piece of data to make a backup copy. In addition it is desirable to prevent a malicious user from making multiples copies from a copy.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cookson et al within the system of Szczutkowski et al because it would allow the system to authorize a one time copy so that a backup can be made of the original piece of data, while preventing illegal subsequent copies from being made from the copy.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan
Examiner
Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100